UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,177	03/26/2004	James F. Riordan	CH920020047US1	2029

7590 09/28/2007

IBM Corporation
Intellectual Property Law Dept.
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/811,177	**Applicant(s)** RIORDAN, JAMES F.	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _26 March 2004_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-22_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-22_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _3/26/04_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. ***Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ogg, et al. (US 7,236,956), and further in view of Scheidt, et al. (7,178,025).***

As per claim 1:

Ogg discloses a method for detecting an attack on a data processing 56system, the method comprising, in the data processing system:

providing an initial secret; (col.22, lines 48 and col.23, lines 46-48)

[binding] the initial secret (col.19, lines 6-18 and col.21, lines 7-14) to data indicative of an initial state of the system via a cryptographic function; (col.23, lines 57-67 and col.24, lines 45-52)

recording state changing administrative actions performed on the system in a log; (col.30, lines 44-47 and col.39, lines 50-52)

prior to performing each state changing administrative action, generating a new secret by performing the cryptographic function on a combination of data indicative of the administrative action and the previous secret (col.19, lines 44-48 and col.20, lines 39-52), and erasing the previous secret; (col.24, lines 58-67)

evolving the initial secret based on the log to produce an evolved secret; comparing the evolved secret with the new secret; (col.33, lines14-19)

determining that the system is uncorrupted if the comparison indicates a match between the evolved secret and the new secret; and (col.33, lines 21-25)

determining that the system in corrupted if the comparison indicates a mismatch between the evolved secret and the new secret. (col.33, lines 38-55)

Ogg suggests private key used by modules to decrypt client secrets transmitted to the module during registration (col.23, lines 57-67 and col.33, lines 15-22), which seems to suggest a form of binding an initial secret to data indicative of an initial state of the system via a cryptographic function (col.19, lines 6-18 and col.21, lines 7-14). However, Ogg did not clearly teach the claimed binding..

Scheidt teaches a system to enforce member access control (to applications) to labeled data with cryptography where this is an improved method of identifying a user for access to a system (col.3, lines 25-44).

Scheidt's invention provides a method of validating a user for access to a system where a validated key is created by binding the factors together to provide authorization data (col.3, lines 60-61 and col.4, lines 2-3). To generate a key includes generating a random value, and binding at least the domain value and the random value together to form this key (col.7, lines 53-55). Scheidt teaches binding can encompass any manner of generating a resultant value from two or more source values in a consistent, repeatable manner (col.19, lines 18-33). Additionally, Scheidt discloses a binder or combiner is the function that produces a (working) key that is used for object encryption, which is to generate a key from shared values (col.26, lines 49-51).

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of Ogg with Scheidt to teach binding an initial secret to data indicative of an initial state of the system via a cryptographic function because a key is generated from two or more (shared) values (col.3, lines 60-61 and col.4, lines 2-3) to validate a user for access to a system (col.19, lines 18-33 and col.26, lines 49-51).

As per claim 2: See Ogg on col.8, lines 10-22; discussing a method as claimed in claim 1, wherein the cryptographic function comprises a one-way hash function.

As per claim 3: See Ogg on col.8, lines 10-29; discussing a method as claimed in claim 2, wherein the hash function comprises an exponentiation function.

As per claim 4: See Ogg on col.7, lines 43-44 and col.23, lines 20-34; discussing a method as claimed in claim 1, wherein the cryptographic function comprises a public/private key pair.

As per claim 5: See Ogg on col.22, lines 65-66; discussing a method as claimed in claim 1, comprising receiving the initial secret from a system administrator.

As per claim 6:

Ogg discloses a data processing system comprising:

a processor; a memory connected to the processor; and (col. 4, lines 62-63 and col.6, lines 23-26)

detection logic connected to the processor and the memory, the detection logic, in use: (col.7, lines 28-42)

providing an initial secret; (col.22, lines 48 and col.23, lines 46-48)

[binding] the initial secret (col.21, lines 7-14 and col.19, lines 6-18) to data indicative of an initial state of the system via a cryptographic function; (col.23, lines 57-67 and col.24, lines 45-52)

recording state changing administrative actions performed on the system in a log; (col.30, lines 44-47 and col.39, lines 50-52)

prior to performing each state changing administrative action, generating a new secret by performing the cryptographic function on a combination of data indicative of the administrative action and the previous secret (col.19, lines 44-48 and col.20, lines 39-52), and erasing the previous secret; (col.24, lines 58-67)

evolving the initial secret based on the log to produce an evolved secret; comparing the evolved secret with the new secret; (col.33, lines14-19)

determining that the system is uncorrupted if the comparison indicates a match between the evolved secret and the new secret; and (col.33, lines 21-25)

determining that the system in corrupted if the comparison indicate a mismatch between the evolved secret and the new secret. (col.33, lines 38-55)

Ogg suggests private key used by modules to decrypt client secrets transmitted to the module during registration (col.23, lines 57-67 and col.33, lines 15-22), which seems to suggest a form of binding an initial secret to data indicative of an initial state of the system via a cryptographic function (col.21, lines 7-14 and col.19, lines 6-18). However, Ogg did not clearly teach the claimed binding.

Scheidt teaches a system to enforce member access control (to applications) to labeled data with cryptography where this is an improved method of identifying a user for access to a system (col.3, lines 25-44). Scheidt's invention provides a method of validating a user for access to a system where a validated key is created by binding the factors together to provide authorization data (col.3, lines 60-61 and col.4, lines 2-3). To generate a key includes generating a random value, and binding at least the domain value and the random value together to form this key (col.7, lines 53-55).

Scheidt teaches binding can encompass any manner of generating a resultant value from two or more source values in a consistent, repeatable manner (col.19, lines 18-33). Additionally, Scheidt discloses a binder or combiner is the function that produces a (working) key that is used for object encryption, which is to generate a key from shared values (col.26, lines 49-51).

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of Ogg with Scheidt to teach binding an initial secret to data indicative of an initial state of the system via a cryptographic function because a key is generated from two or more (shared) values (col.3, lines 60-61 and col.4, lines 2-3) to validate a user for access to a system (col.19, lines 18-33 and col.26, lines 49-51).

As per claim 7: See Ogg on col.8, lines 10-22; discussing a system as claimed in claim 6, wherein the cryptographic function comprises a one-way hash function.

As per claim 8: See Ogg on col.8, lines 10-29; discussing a system as claimed in claim 7, wherein the hash function comprises an exponentiation function.

As per claim 9: See Ogg on col.7, lines 43-44 and col.23, lines 20-34; discussing a system as claimed in claim 6, wherein the cryptographic function comprises a public/private key pair.

As per claim 10: See Ogg on col.7, lines 28-42***;*** discussing a system as claimed in claim 6, wherein the detector logic receives the initial secret from a system administrator.

As per claim 11: See Ogg on col. 4, lines 62-63 and col.6, lines 23-26; discussing a computer program element comprising computer program code means which, when loaded in a processor of a computer system, configures the processor to perform a method as claimed in claim 1.

As per claim 12: See Ogg on col. 4, lines 62-63 and col.6, lines 23-26; discussing an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing detection of an attack on a data processing system, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

As per claim 13: See Ogg on col.7, lines 28-45 and col.24, lines 15-16; discussing a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting an attack on a data processing system, said method steps comprising the steps of claim 1.

As per claim 14: See Ogg on col. 4, lines 62-63 and col.6, lines 23-26; discussing a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a data processing system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 6.

As per claim 15:

Ogg discloses a method for cryptographic entangling of state and administration in a data processing system, the method comprising:

initializing the system by generating an initial secret releasing (col.22, lines 48 and col.23, lines 46-48) *[binding]* data; (col.21, lines 7-14 and col.19, lines 6-18)

[binding the binding] data to the initial secret; (col.23, lines 57-67 and col.24, lines 45-52)

updating the initial secret in advance of an administrative action by computing a new secret; (col.4, lines 46-50 and col.19, lines 44-48 and col.20, lines 39-52)

erasing the initial secret together with any information from which the initial secret might be derived; (col.24, lines 58-67)

recording data indicative of the administrative action; (col.30, lines 44-47 and col.39, lines 50-52)

permitting execution of the administrative action; (col.14, lines 48-50 and col.24, lines 22-30)

offering a proof that the new secret corresponds to the initial secret as it has evolved according to a record of administrative actions. (col.33, lines 14-55)

Ogg suggests private key used by modules to decrypt client secrets transmitted to the module during registration (col.23, lines 57-67 and col.33, lines 15-22), which seems to suggest a form of binding an initial secret to data indicative of an initial state of the system via a cryptographic function (col.21, lines 7-14 and col.19, lines 6-18). However, Ogg did not clearly teach the claimed binding.

Scheidt teaches a system to enforce member access control (to applications) to labeled data with cryptography where this is an improved method of identifying a user for access to a system (col.3, lines 25-44). Scheidt's invention provides a method of validating a user for access to a system where a validated key is created by binding the factors together to provide authorization data (col.3, lines 60-61 and col.4, lines 2-3). To generate a key includes generating a random value, and binding at least the domain value and the random value together to form this key (col.7, lines 53-55). Scheidt teaches binding can encompass any manner of generating a resultant value from two or more source values in a consistent, repeatable manner (col.19, lines 18-33). Additionally, Scheidt discloses a binder or combiner is the function that produces a (working) key that is used for object encryption, which is to generate a key from shared values (col.26, lines 49-51).

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of Ogg with Scheidt to teach binding an initial secret to data indicative of an initial state of the system via a cryptographic function because a key is generated from two or more (shared) values (col.3, lines 60-61 and col.4, lines 2-3) to validate a user for access to a system (col.19, lines 18-33 and col.26, lines 49-51).

As per claim 16: as rejected in claim 15; discussing a method as recited in claim 15, wherein the step of offering retrieves the initial secret via a request for entry of the initial secret by a system administrator, retrieving the record of administrative actions previous stored; and evolving a candidate secret for the initial secret based on the record of administrative actions retrieved; comparing the candidate secret with a current secret; if the candidate secret matches the current secret, reporting that the data processing system is still in an uncorrupted state, and if the candidate secret does not match the current secret, reporting that the data processing system is in a potentially compromised state.

As per claim 17: See Ogg on col.7, lines 28-45 and col.24, lines 15-16; discussing a method as recited in claim 15, further comprising permitting detection of any Trojan horse within the system.

As per claim 18: See Ogg on col.22, lines 48 and col.23, lines 46-48; discussing a method as recited in claim 15, wherein the initial secret is supplied via a secure communication channel.

As per claim 19: See Ogg on Scheidt on col.19, lines 18-33 and col.26, lines 49-51; discussing a method as recited in claim 15, wherein the binding data takes different forms depending on the data processing system, an application of the data processing system, and a trust mechanisms associated with communication of the initial secret.

As per claim 20: See Ogg on col.4, lines 46-50 and col.21, lines 4-26 and col.25, lines 20-55; discussing a method as recited in claim 15, wherein the administrative action is an action taken from a group of actions consisting of: updating of system executable code; updating of system libraries; installation of kernel modules; reading of files such as those used to store system states during rebooting operations; alteration of configuration files; alteration of system run-level codes; writing to or reading from peripheral devices; and any combination of these actions.

As per claim 20: See Ogg on col.19, lines 6-18***;*** discussing a method as recited in claim 15, wherein the step of computing the new secret includes applying a one way function to a combination of a previous secret and data indicative of the administrative action.

As per claim 21: See Ogg on col. 4, lines 62-63 and col.6, lines 23-26; discussing an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing cryptographic entanglement of state and administration in a data processing system, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 15.

As per claim 22: See Ogg on col. 4, lines 62-63 and col.6, lines 23-26; discussing a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for cryptographic entangling of state and administration in a data processing system, said method steps comprising the steps of claim 15.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100